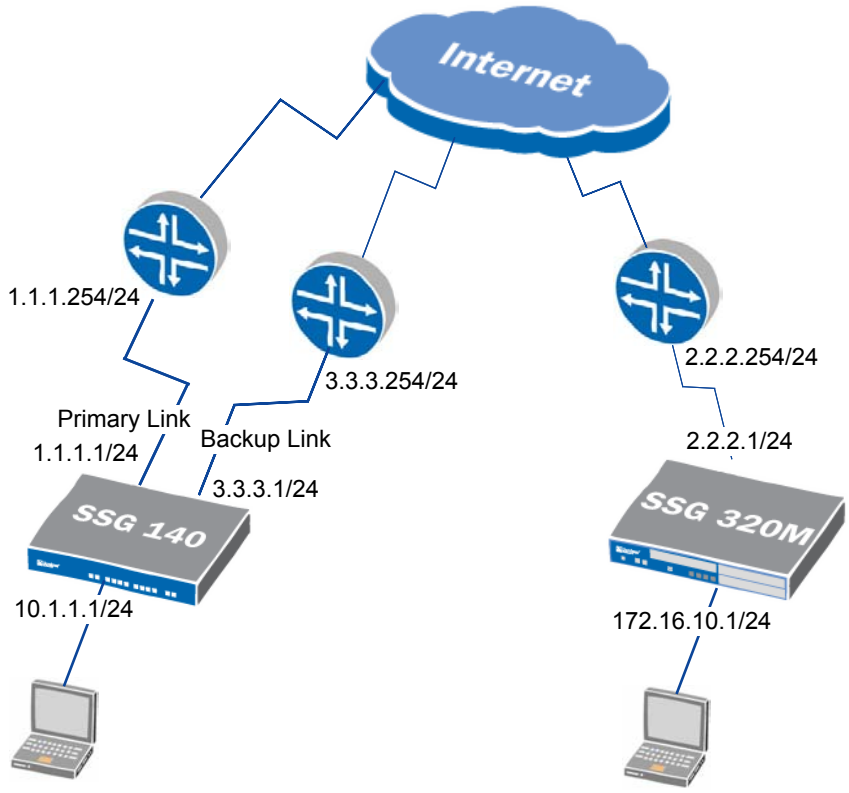
Interface Failover with Route Based VPNs

Version 1.4

Purpose
This paper describes how to configure VPN and Interface Failover using Juniper Firewall devices, NS-25, NS-50, NS-204, NS-208, SSG-140, SSG-320M, SSG-350M, SSG-520M, and SSG-550M. The failover mechanism is different than the Untrust Failover feature on the NetScreen-5GT platforms, or the Backup interface feature on the SSG-5 and SSG-20. We will discuss the general procedure of setting this up.

This article includes an example using an SSG-140 with Interface failover, but it also applies to the firewall devices listed above, running ScreenOS 5.1.0 and higher.

Example



The best way to discuss the interface failover and VPN is to make use of an example.

In this example, the SSG-140 is configured with a network of 10.1.1.0/24 in the trust zone. The primary untrust interface is 1.1.1.1/24, and when that interface fails, the backup connection will take over with an IP of 3.3.3.1/24. This example will use track-ip for interface monitoring.

Interface Failover with SSG-140:

This example will describe procedures for interface failover for the SSG-140, but the same concept would apply to NS-25, NS-50, SSG140, SSG320, SSG-320M, SSG-350M, SSG-520, SSG-520M, SSG-550, and SSG-550M. The interface failover mechanism is done via the interface monitoring feature.

With Interface Monitoring, weighted sum of track-ip failures are compared to a set track-ip threshold. Once the weighted sum of track-ip failures meets or exceeds the track-ip threshold, an interface track-ip failure weight is assigned. The interface track-ip failure weight is then compared to the interface threshold. If the interface track-ip failure weight meets or exceeds the interface monitor threshold, the interface turns to a failed state.

Configure Interfaces

First, you'll need to configure two interfaces in the untrust zone. We will choose ethernet0/2 and ethernet0/3:

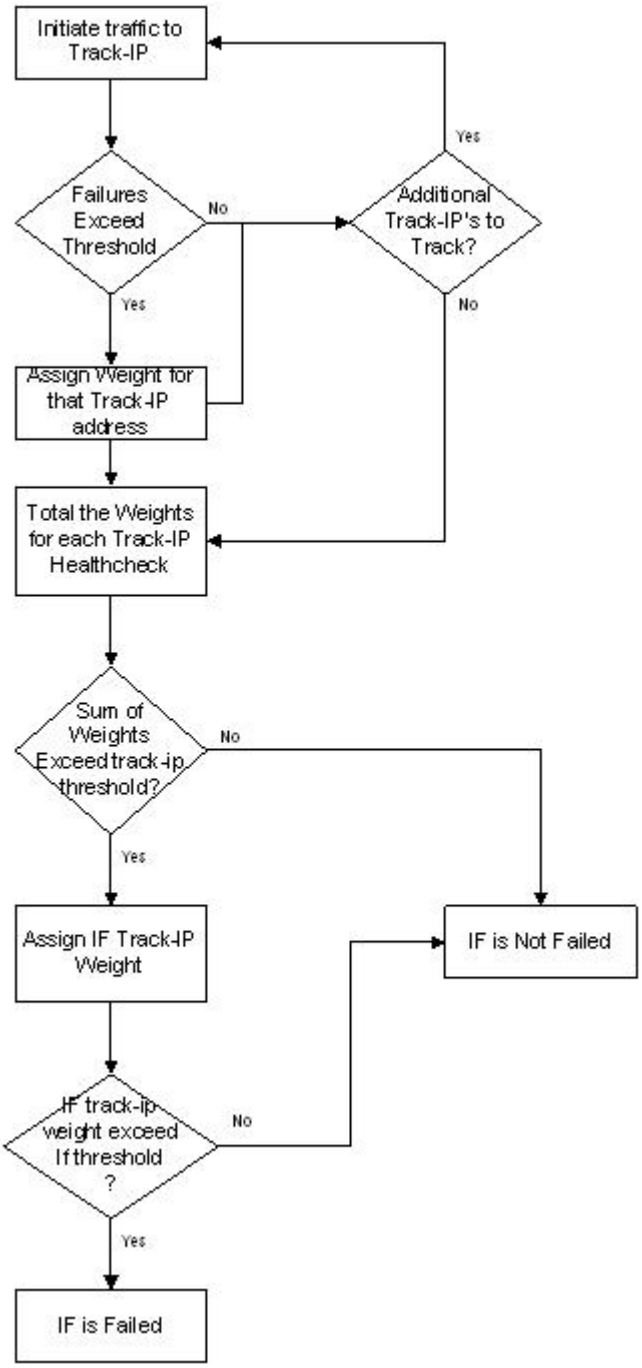
```
set interface "ethernet0/2" zone "Untrust"
set interface ethernet0/2 ip 1.1.1.1/24
set interface "ethernet0/3" zone "Untrust"
set interface ethernet0/3 ip 3.3.3.1/24
```

Interface Monitoring Using Track-IP

You can monitor the state of the primary interface by using one or more track-ip address(s). The interface sends an ICMP packet to the specified track-ip at specified intervals. If the ICMP request to the track-ip fails, this is counted as one ping failure. If the total ping failures reach the threshold amount (which you configure), a weight for that track-ip failure is assigned (based on what you configure).

A sum of all track-ip failure weights is calculated. If the sum of the track-ip failure weights meets or exceeds the specified threshold, another weight is assigned to the weighted sum. If this weight meets or exceeds the interface threshold, the interface will go down.

This is illustrated in the flowchart below:



In our example, interface failover configuration for interface ethernet0/2 is as follows:

```
set interface ethernet0/2 monitor track-ip ip
set interface ethernet0/2 monitor track-ip threshold 100
set interface ethernet0/2 monitor track-ip weight 50
set interface ethernet0/2 monitor track-ip ip 2.2.2.100 weight 50
set interface ethernet0/2 monitor track-ip ip 2.2.2.10 weight 60
set interface ethernet0/2 monitor threshold 40
```

In this example, an ICMP is sent from interface ethernet0/2 to 2.2.2.100 and 2.2.2.10. One ICMP is every second. The default failure count threshold is 3. If there are 3 consecutive failed responses to the ICMP attempts, a track-ip weight for 2.2.2.100 of 50 is assigned. The track-ip weights are compared to the track-ip threshold, which is 100. Since 50 < 100, the track-ip for this interface has not failed yet. However, if the track-ip ICMP's to 198.6.1.3 fails 3 times, the track-ip weight for 2.2.2.10 of 60 is assigned. The sum of the track-ip weights is then 110, which is greater than 100. Therefore, the track-ip is in a failed condition, and the interface track-ip weight of 50 is assigned. This track-ip weight is then compared to the interface monitor threshold, which is 40. If this is the case, the interface is then set to failed condition, and the interface will go in down state.

NOTE: A simple Interface Failover configuration example using the default weights and thresholds is provided in the following article: http://kb.juniper.net/KB8704.

You can check the condition of the interface monitoring by issuing the command

```
get interface ethernet0/2 monitor
```

To check the condition of each interface track-ip ip address:

```
ssg140-> get interface ethernet0/2 track-ip ip
ip address           intval threshold wei gateway         fail-count success
2.2.2.100                 1         3  50 0.0.0.0                 0 77%
2.2.2.10                  1         3  60 0.0.0.0                 0 100%
failure weight: 50, threshold: 100, not failed: 0 ip(s) failed, weighted sum = 0
```

To check the condition of the interface monitoring:

```
ssg140-> get interface ethernet0/2 monitor
 interface ethernet0/2 monitoring threshold: 40, failure action: interface
logically down, weighted sum: 0, not failed
interface ethernet0/2 monitor interfaces:
interface ethernet0/2 monitor zones:
```

Here is a sample where the interface failed over due to track-ip failures:

```
ssg140-> get interface ethernet0/2 monitor track-ip
ip address           intval threshold wei gateway         fail-count success
2.2.2.100                 1         3  50 0.0.0.0                63 77%
2.2.2.10                  1         3  60 0.0.0.0                63 88%
failure weight: 50, threshold: 100, failed: 2 ip(s) failed, weighted sum = 110
ssg140-> get interface ethernet0/2 monitor
interface ethernet0/2 monitoring threshold: 40, failure action: interface
logically down, weighted sum: 50, failed
interface ethernet0/2 monitor interfaces:
interface ethernet0/2 monitor zones:
```

Here, the weighted sum is 110, which exceeds the threshold 100. A failure weight of 50 has been assigned. This failure weight is then compared to the interface monitor threshold, which is 40. The failure weight exceeds the interface monitor threshold, and therefore the interface has failed.

When interface ethernet0/2 is restored, it will regain it's physical link up status, due to the track-ip monitor threshold tests/comparisons.

Configuring Redundant VPN with Interface Failover

To configure VPNs to follow the interface (no matter if it fails over or not), route based VPN configuration is required. One set of IKE gateways are required for each outgoing interface (i.e. one VPN tunnel for primary, one VPN tunnel for backup outgoing interface).

On the peer gateway, there will also be two sets of VPN tunnels to the SSG140 (one for primary, and one for backup). We will configure the VPNs according to the table below:

SSG-140:

IKE Gateway	Gateway Address	P1 Proposal	Outgoing-if	P2 Proposal	Local Proxy-id	Remote Proxy-id	tunnel-if
Primary	2.2.2.1	Compatible	ethernet0/2	Compatible	10.1.1.0/24	172.16.10.0/24	tunnel.1
Backup	2.2.2.1	Compatible	ethernet0/3	Compatible	10.1.1.0/24	172.16.10.0/24	tunnel.2

SSG-320M:

IKE Gateway	Gateway Address	P1 Proposal	Outgoing-if	P2 Proposal	Local Proxy-id	Remote Proxy-id	tunnel-if
Primary	1.1.1.1	Compatible	ethernet0/2	Compatible	10.1.1.0/24	172.16.10.0/24	tunnel.1
Backup	3.3.3.1	Compatible	ethernet0/2	Compatible	10.1.1.0/24	172.16.10.0/24	tunnel.2

The equivalent VPN configurations for each device is shown below

SSG-140:

```
set interface "tunnel.1" zone "Untrust"
set interface "tunnel.2" zone "Untrust"
set interface tunnel.1 ip unnumbered interface ethernet0/2
set interface tunnel.2 ip unnumbered interface ethernet0/3
set ike gateway "ssg320gw primary" address 2.2.2.1 Main outgoing-interface "ethernet0/2"
preshare "XF3N5aRHNH6n3KsVh4CnxKpF4nnCdiBCiw==" sec-level standard
set ike gateway "ssg320gw backup" address 2.2.2.1 Main outgoing-interface "ethernet0/3"
preshare "ITBkIkGGNe7AuOsZ04CBvEKvQunnk42FKA==" sec-level standard
set vpn "ssg320vpn primary" gateway " ssg320gw primary" no-replay tunnel idletime 0 sec-
level standard
set vpn " ssg320vpn primary " monitor optimized rekey
set vpn " ssg320vpn primary " id 3 bind interface tunnel.1
set vpn "ssg320vpn backup" gateway " ssg320gw backup " no-replay tunnel idletime 0 sec-
level standard
set vpn "ssg320vpn backup" monitor optimized rekey
set vpn "ssg320vpn backup" id 2 bind interface tunnel.2
set vpn "ssg320vpn primary" proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 "ANY"
set vpn "ssg320vpn backup" proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 "ANY"
```

SSG-320M:

```
set interface "tunnel.1" zone "Untrust"
set interface "tunnel.2" zone "Untrust"
set interface tunnel.1 ip unnumbered interface ethernet0/2
set interface tunnel.2 ip unnumbered interface ethernet0/2
set ike gateway "ssg140gw primary" address 3.3.3.1 Main outgoing-interface "ethernet0/2"
preshare "7IdjSGXsNaD+jFsKKECjMI+YoEnL6AIo3w==" sec-level standard
set ike gateway "ssg140gw backup" address 1.1.1.1 Main outgoing-interface "ethernet0/2"
preshare "4xoSwfrMNJqhzxs6xPCGiuCIginE8DWo3A==" sec-level standard
set ike respond-bad-spi 1
set vpn "ssg140vpn primary" gateway "ssg140gw primary" no-replay tunnel idletime 0 sec-
level standard
set vpn " ssg140vpn primary " monitor optimized rekey
set vpn " ssg140vpn primary " id 1 bind interface tunnel.1
set vpn "ssg140vpn backup" gateway " ssg140gw backup " no-replay tunnel idletime 0 sec-
level standard
set vpn " ssg140vpn backup " monitor optimized rekey
set vpn " ssg140vpn backup " id 2 bind interface tunnel.2
set vpn " ssg140vpn primary " proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24
"ANY"
set vpn " ssg140vpn backup " proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24 "ANY"
```

Routing Considerations

When the primary link is up, we want all traffic to route through interface ethernet0/2. We only want traffic to go through ethernet0/3 when the ethernet0/2 link goes down. Therefore, we separate these by setting a lower metric on the backup route for both default route and for tunnel routes. Also, avoid using permanent routes, as this would prevent route failovers to work.

SSG140:

```
set route  0.0.0.0/0 interface ethernet0/2 gateway 1.1.1.254
set route  0.0.0.0/0 interface ethernet0/3 gateway 3.3.3.254 metric 10
set route  172.16.10.0/24 interface tunnel.1
set route  172.16.10.0/24 interface tunnel.2
```

Routing Table of SSG140 when Primary is up:

```
IPv4 Dest-Routes for <untrust-vr> (0 entries)
------------------------------------------------------------------------------------------
H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
N: NHRP
iB: IBGP eB: EBGP O: OSPF E1: OSPF external type 1
E2: OSPF external type 2 trailing B: backup route


IPv4 Dest-Routes for <trust-vr> (13 entries)
------------------------------------------------------------------------------------------
         ID           IP-Prefix      Interface         Gateway   P Pref    Mtr      Vsys
------------------------------------------------------------------------------------------
*         7         1.1.1.1/32         eth0/2         0.0.0.0   H    0      0      Root
*        15          0.0.0.0/0         eth0/2       1.1.1.254   S   20      1      Root
         17          0.0.0.0/0         eth0/3       3.3.3.254   S   20     10      Root
*         9         3.3.3.1/32         eth0/3         0.0.0.0   H    0      0      Root
*        11        10.1.1.1/32         eth0/0         0.0.0.0   H    0      0      Root
*        18     172.16.10.0/24          tun.1         0.0.0.0   S   20      1      Root
         19     172.16.10.0/24          tun.2         0.0.0.0   S   20      1      Root
*         5        172.0.0.0/8         eth0/1     172.19.50.1   S   20      1      Root
*         3     172.19.50.0/23         eth0/1         0.0.0.0   C    0      0      Root
*         4    172.19.51.14/32         eth0/1         0.0.0.0   H    0      0      Root
*        10        10.1.1.0/24         eth0/0         0.0.0.0   C    0      0      Root
*         8         3.3.3.0/24         eth0/3         0.0.0.0   C    0      0      Root
*         6         1.1.1.0/24         eth0/2         0.0.0.0   C    0      0      Root
```

Routing Table of SSG140 when Backup (e4) is Up and Primary (e3) is Down:

```
IPv4 Dest-Routes for <untrust-vr> (0 entries)
------------------------------------------------------------------------------------------
H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
N: NHRP
iB: IBGP eB: EBGP O: OSPF E1: OSPF external type 1
E2: OSPF external type 2 trailing B: backup route


IPv4 Dest-Routes for <trust-vr> (13 entries)
------------------------------------------------------------------------------------------
         ID           IP-Prefix      Interface         Gateway   P Pref    Mtr      Vsys
------------------------------------------------------------------------------------------
*         7         1.1.1.1/32         eth0/2         0.0.0.0   H    0      0      Root
         15          0.0.0.0/0         eth0/2       1.1.1.254   S   20      1      Root
*        17          0.0.0.0/0         eth0/3       3.3.3.254   S   20     10      Root
*         9         3.3.3.1/32         eth0/3         0.0.0.0   H    0      0      Root
*        11        10.1.1.1/32         eth0/0         0.0.0.0   H    0      0      Root
         18     172.16.10.0/24          tun.1         0.0.0.0   S   20      1      Root
*        19     172.16.10.0/24          tun.2         0.0.0.0   S   20      1      Root
*         5        172.0.0.0/8         eth0/1     172.19.50.1   S   20      1      Root
*         3     172.19.50.0/23         eth0/1         0.0.0.0   C    0      0      Root
*         4    172.19.51.14/32         eth0/1         0.0.0.0   H    0      0      Root
*        10        10.1.1.0/24         eth0/0         0.0.0.0   C    0      0      Root
*         8         3.3.3.0/24         eth0/3         0.0.0.0   C    0      0      Root
*         6         1.1.1.0/24         eth0/2         0.0.0.0   C    0      0      Root
```

Security Associations Table:

With primary link active, the SA on the SSG140 side will look like the following:

```
SSG140-> get sa
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001<         2.2.2.1  500 esp:3des/sha1 0afcffd7  2160 unlim A/U    -1 0
00000001>         2.2.2.1  500 esp:3des/sha1 3d982f16  2160 unlim A/U    -1 0
00000002<         2.2.2.1  500 esp:3des/sha1 00000000 expir unlim I/I    -1 0
00000002>         2.2.2.1  500 esp:3des/sha1 00000000 expir unlim I/I    -1 0
ssg140->
```

The SA on the SSG320 side will look like the following:

```
SSG320-> get sa
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001< 3.3.3.1          500 esp:3des/sha1 00000000 expir unlim I/I    -1 0
00000001> 3.3.3.1          500 esp:3des/sha1 00000000 expir unlim I/I    -1 0
00000002< 1.1.1.1          500 esp:3des/sha1 3d982f16  2160 unlim A/U    -1 0
00000002> 1.1.1.1          500 esp:3des/sha1 0afcffd7  2160 unlim A/U    -1 0
ns5gt->
```

After failover, the SA on the SSG140 side will look like the following:

```
SSG140-> get sa
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001<         2.2.2.1  500 esp:3des/sha1 0afcffd7  1929 unlim A/U    -1 0
00000001>         2.2.2.1  500 esp:3des/sha1 3d982f16  1929 unlim A/U    -1 0
00000002<         2.2.2.1  500 esp:3des/sha1 0afcffd8  3564 unlim A/U    -1 0
00000002>         2.2.2.1  500 esp:3des/sha1 3d982f17  3564 unlim A/U    -1 0
ssg140->
```

The SA on the SSG320 side will look like the following:

```
SSG320-> get sa
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001< 3.3.3.1          500 esp:3des/sha1 3d982f17  3562 unlim A/U    -1 0
00000001> 3.3.3.1          500 esp:3des/sha1 0afcffd8  3562 unlim A/U    -1 0
00000002< 1.1.1.1          500 esp:3des/sha1 3d982f16  1926 unlim A/U    -1 0
00000002> 1.1.1.1          500 esp:3des/sha1 0afcffd7  1926 unlim A/U    -1 0
```

Question: Why are there SA's active on both VPN tunnels?
Answer: Since this is a route based VPN, determination on if a VPN tunnel is up is based on the healthchecks due to the VPN Monitor mechanism. The defaults for VPNMonitor healthcheck is the following:

```
SSG140-> get vpnmonitor
Vpn monitor interval : 10(seconds)
Vpn monitor threshold: 10
SSG140->
```

This means one VPN monitor healthcheck packet is sent every 10 seconds. The VPN failure threshold is set to 10, so it would take 100 seconds before the SA would be marked down. This would also account for no VPN traffic response until 100 seconds after the interface failover occurred.

It is recommended to modify the VPNMonitor settings so that the SA would mark itself down in a shorter timeframe. If you choose an interval of 2 seconds, and a threshold of 2, the SA would mark itself down 4 seconds after interface failover occurs.

```
SSG140-> set vpnmonitor threshold 2
SSG140-> set vpnmonitor interval 2
SSG140-> get vpnmonitor
Vpn monitor interval : 2(seconds)
Vpn monitor threshold: 2
SSG140->
```

Caution: Using the lowest interval and threshold may cause the VPN to go down before it actually should be. You should tweak this value after several trial and error cycles.

After the SA's bound to the inactive interface marks itself down, the get sa on each side of the tunnel will look like the following:

SSG140:

```
SSG140-> get sa
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001<         2.2.2.1  500 esp:3des/sha1 0afcffd7  1209 unlim I/I    -1 0
00000001>         2.2.2.1  500 esp:3des/sha1 3d982f16  1209 unlim I/I    -1 0
00000002<         2.2.2.1  500 esp:3des/sha1 0afcffd8  2844 unlim A/U    -1 0
00000002>         2.2.2.1  500 esp:3des/sha1 3d982f17  2844 unlim A/U    -1 0
ssg140->
```

SSG320:

```
SSG320-> get sa
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001< 3.3.3.1          500 esp:3des/sha1 3d982f17  2843 unlim A/U    -1 0
00000001> 3.3.3.1          500 esp:3des/sha1 0afcffd8  2843 unlim A/U    -1 0
00000002< 1.1.1.1          500 esp:3des/sha1 3d982f16  1207 unlim I/I    -1 0
00000002> 1.1.1.1          500 esp:3des/sha1 0afcffd7  1207 unlim I/I    -1 0
```

Configuration for SSG140:

```
SSG140-> get config
Total Config size 5618:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Trust"
set interface "ethernet0/1" zone "DMZ"
set interface "ethernet0/2" zone "Untrust"
set interface "ethernet0/3" zone "Untrust"
set interface "tunnel.1" zone "Untrust"
set interface "tunnel.2" zone "Untrust"
set interface ethernet0/0 ip 10.1.1.1/24
set interface ethernet0/0 nat
unset interface vlan1 ip
set interface ethernet0/1 ip 172.19.51.14/23
set interface ethernet0/1 nat
set interface ethernet0/2 ip 1.1.1.1/24
set interface ethernet0/2 route
set interface ethernet0/3 ip 3.3.3.1/24
set interface ethernet0/3 route
set interface tunnel.1 ip unnumbered interface ethernet0/2
set interface tunnel.2 ip unnumbered interface ethernet0/3
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/1 ip manageable
set interface ethernet0/2 ip manageable
set interface ethernet0/3 ip manageable
set interface ethernet0/1 manage ssh
set interface ethernet0/1 manage telnet
set interface ethernet0/1 manage snmp
set interface ethernet0/1 manage ssl
set interface ethernet0/1 manage web
set interface ethernet0/1 manage mtrace
set interface ethernet0/2 manage ping
```

```
set interface ethernet0/2 manage ssh
set interface ethernet0/2 manage telnet
set interface ethernet0/2 manage snmp
set interface ethernet0/2 manage ssl
set interface ethernet0/2 manage web
set interface ethernet0/2 manage mtrace
set interface ethernet0/3 manage ping
set interface ethernet0/3 manage ssh
set interface ethernet0/3 manage telnet
set interface ethernet0/3 manage snmp
set interface ethernet0/3 manage ssl
set interface ethernet0/3 manage web
set interface ethernet0/3 manage mtrace
set interface ethernet0/2 monitor track-ip ip
set interface ethernet0/2 monitor track-ip threshold 100
set interface ethernet0/2 monitor track-ip weight 50
set interface ethernet0/2 monitor track-ip ip 2.2.2.10 weight 50
set interface ethernet0/2 monitor track-ip ip 2.2.2.1 weight 60
unset interface ethernet0/2 monitor track-ip dynamic
set interface ethernet0/2 monitor threshold 40
unset flow no-tcp-seq-check
set flow tcp-syn-check
unset flow tcp-syn-bit-check
set flow reverse-route clear-text prefer
set flow reverse-route tunnel always
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set ike gateway "ssg320gw primary" address 2.2.2.1 Main outgoing-interface "ethernet0/2"
preshare "XF3N5aRHNH6n3KsVh4CnxKpF4nnCdiBCiw==" sec-level standard
set ike gateway "ssg320gw backup" address 2.2.2.1 Main outgoing-interface "ethernet0/3"
preshare "ITBkIkGGNe7AuOsZ04CBvEKvQunnk42FKA==" sec-level standard
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vpn "ssg320vpn primary" gateway "ssg320gw primary" no-replay tunnel idletime 0 sec-
level standard
set vpn "ssg320vpn primary" monitor optimized rekey
set vpn "ssg320vpn primary" id 3 bind interface tunnel.1
set vpn "ssg320vpn backup" gateway "ssg320gw backup" no-replay tunnel idletime 0 sec-
level standard
set vpn "ssg320vpn backup" monitor optimized rekey
set vpn "ssg320vpn backup" id 2 bind interface tunnel.2
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
set url protocol websense
exit
set vpn "ssg320vpn primary" proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 "ANY"
set vpn "ssg320vpn backup" proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 "ANY"
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set config lock timeout 5
unset license-key auto-update
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 172.0.0.0/8 interface ethernet0/1 gateway 172.19.50.1
set route 0.0.0.0/0 interface ethernet0/2 gateway 1.1.1.254
set route 0.0.0.0/0 interface ethernet0/3 gateway 3.3.3.254 metric 10
set route 172.16.10.0/24 interface tunnel.1
set route 172.16.10.0/24 interface tunnel.2 metric 10
exit
```

```
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```

Configuration for SSG320:

```
SSG320M-> get config
Total Config size 4620:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Trust"
set interface "ethernet0/1" zone "DMZ"
set interface "ethernet0/2" zone "Untrust"
set interface "ethernet0/3" zone "Untrust"
set interface "tunnel.1" zone "Untrust"
set interface "tunnel.2" zone "Untrust"
set interface ethernet0/0 ip 192.168.1.1/24
set interface ethernet0/0 nat
unset interface vlan1 ip
set interface ethernet0/1 ip 172.19.51.44/23
set interface ethernet0/1 nat
set interface ethernet0/2 ip 2.2.2.1/24
set interface ethernet0/2 route
set interface tunnel.1 ip unnumbered interface ethernet0/2
set interface tunnel.2 ip unnumbered interface ethernet0/2
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/1 ip manageable
set interface ethernet0/2 ip manageable
set interface ethernet0/2 manage ping
set interface ethernet0/2 manage ssh
set interface ethernet0/2 manage telnet
set interface ethernet0/2 manage snmp
set interface ethernet0/2 manage ssl
set interface ethernet0/2 manage web
set interface ethernet0/2 manage mtrace
```

```
unset flow no-tcp-seq-check
set flow tcp-syn-check
unset flow tcp-syn-bit-check
set flow reverse-route clear-text prefer
set flow reverse-route tunnel always
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set ike gateway "ssg140gw primary" address 3.3.3.1 Main outgoing-interface "ethernet0/2"
preshare "7IdjSGXsNaD+jFsKKECjMI+YoEnL6AIo3w==" sec-level standard
set ike gateway "ssg140gw backup" address 1.1.1.1 Main outgoing-interface "ethernet0/2"
preshare "4xoSwfrMNJqhzxs6xPCGiuCIginE8DWo3A==" sec-level standard
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vpn "ssg140vpn primary" gateway "ssg140gw primary" no-replay tunnel idletime 0 sec-
level standard
set vpn "ssg140vpn primary" monitor optimized rekey
set vpn "ssg140vpn primary" id 1 bind interface tunnel.1
set vpn "ssg140vpn backup" gateway "ssg140gw backup" no-replay tunnel idletime 0 sec-
level standard
set vpn "ssg140vpn backup" monitor optimized rekey
set vpn "ssg140vpn backup" id 2 bind interface tunnel.2
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
set url protocol websense
exit
set vpn "ssg140vpn primary" proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24 "ANY"
set vpn "ssg140vpn backup" proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24 "ANY"
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set config lock timeout 5
unset license-key auto-update
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 172.0.0.0/8 interface ethernet0/1 gateway 172.19.50.1
set route 3.3.3.0/24 interface ethernet0/2 gateway 2.2.2.254
set route 1.1.1.0/24 gateway 2.2.2.254
set route 10.1.1.0/24 interface tunnel.1
set route 10.1.1.0/24 interface tunnel.2
set route 0.0.0.0/0 interface ethernet0/2 gateway 2.2.2.254
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```